



Number: CSB-130724-1

Released: 24 July 2013

Modified:

Subject: FortiClient AV update package causes connectivity issues

Product: FortiClient

Description of Issue:

AntiVirus signature update package version 17.940 was released through the FortiGuard network on July 19, 2013. Once installed by FortiClient, a false positive on a Microsoft file named "*tcpip.sys*" is detected during a scheduled scan. FortiClient identifies the file as a virus and quarantines it, which causes the network driver of the PC to stop working.

Affected Products:

FortiClient 5.0.0 through to 5.0.4

Affected OS:

Windows – All versions

Resolution:

A correction for the false positive behavior has been made with AV signature update package version 17.943 and released through FortiGuard on July 22, 2013.

Determine if your PC is affected:

1. Open the FortiClient Console, click on AntiVirus, click on the "Threats Quarantined" link.
2. Search for an entry in the list that matches "*tcpip.sys*". There may be more than one entry.

Restore your PC:

1. Download the TCPIP-fix.zip file from the following location and copy to a USB flash drive or similar media:

ftp://ftp-temp:r3triv3@support.fortinet.com/dropbox/CSB_Forticlient_17.940/TCPIP-fix.zip

2. Disable the "Real Time Protection" from the FortiClient Console.
3. Shutdown the FortiClient software.
4. Open the cmd prompt with "Run As Administrator" privilege.
5. Perform the command **"net stop fortishield"**.
6. Transfer the TCPIP-fix.zip to the workstation from the USB flash.
7. Extract TCPIP-fix.zip into a folder.
8. Using the command line interface, browse to the extracted folder.
9. Perform **"runme.bat"** and wait for the script to finish. You will see the following message in the CMD window:
Please reboot when Windows reports that it has finished installing adapters.
Press any key to continue . . .
10. In the Windows tray, you will see a message **"Installing device driver software"** and then a second message **"Your device is ready to use"**.
11. Reboot the PC.
12. After the reboot and the network is restored, update the FortiClient AV signatures.
13. Re-enable "Real Time Protection" from the FortiClient Console.

Note: Please use the following link to retrieve the TCPIP-fix.zip file:

ftp://ftp-temp:r3triv3@support.fortinet.com/dropbox/CSB_Forticlient_17.940/TCPIP-fix.zip

Technical Support Contact Information: http://www.fortinet.com/support/contact_support.html
Fortinet technical support home page: <https://support.fortinet.com>

All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Statements contained herein were attained in internal lab tests under ideal conditions, and performance may vary; network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all representations and warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with an express representation or warranty included therein. All Fortinet end-customers are bound by the terms of Fortinet's current End User License Agreement. The information in this Customer Support Bulletin is provided for remedial purposes and is designed to assist customers in corrective action that may be helpful to the customer.